CEA ACTION PROPOSAL

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

A. GENERAL INFORMATION

1. Date: 09/08/2022

2. Department: State Treasurer's Office (STO)

3. Organizational Placement (Division/Branch/Office Name)

Executive Office

4. CEA Position Title

Enterprise Risk and Compliance Officer (ERCO)

5. Summary of proposed position description and how it relates to the program's mission or purpose. (*2-3 sentences)*

The Enterprise Risk and Compliance Officer (CEA) will directly report to the Chief Deputy Treasurer. The ERCO will allow for an enterprise-wide risk assessment process that includes developing a risk management strategy, policies, procedures, and tools; monitoring and reporting risk, as well as oversight of the enterprise-wide risk assessment process. An ERCO will help management to engage in proactive and adequate monitoring of risks of the STO's day to day operations and regulatory oversight of the organization.

6. Reports to: (*Class Title/Level*)

Chief Deputy Treasurer

7. Relationship with Department Director (*Select one)*

☑ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.

☐ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(*Explain*):

8. Organizational Level *(Select one)*

☐ 1st ☑ 2nd ☐ 3rd ☐ 4th ☐ 5th (mega departments only - 17,001+ allocated positions)

B. SUMMARY OF REQUEST

9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

The Enterprise Risk and Compliance Officer (ERCO) will report directly to the Chief Deputy Treasurer, both functionally and administratively and will be responsible for assisting with the development of a governance risk management strategy to identify, evaluate, mitigate, and monitor the State Treasurer's Office's (STO) operational and strategic risk and risk management tools, practices, and policies. The ERCO will assist the STO, and the Boards, Commissions, and Authorities (BCA) under its purview, in the evaluation of enterprise risk, development of risk mitigation plans, compliance tracking of regulations and laws with respect to reporting and compliance with control agencies and the Legislature as well as coordination on all externally performed audits and addressing areas with control deficiencies. The compliance functions of the ERCO will include making recommendations on standards and procedures in identifying, preventing, detecting, and correcting noncompliance with applicable rules and regulations. Additionally, the ERCO will coordinate and serve as the STO's liaison for external audits. The ERCO will assist management in verifying internal controls in those areas with audit findings and assist with developing risk mitigation strategies. Furthermore, this position will be able to track and monitor compliance with prior and future audit recommendations to ensure they are addressed with appropriate remediation, thereby reducing risk to the STO and its BCAs.

The duties of the ERCO include developing a risk management strategy, policies, procedures, and tools; monitoring and reporting risk, as well as oversight of the enterprise-wide risk assessment process. Specifically, it will require assisting management with the creation of a risk framework that identifies, analyzes, evaluates, treats, monitors, and reviews, along with a risk mitigation strategy that will result in a better risk aggregation process across the organization. Additionally, the ERCO would help the STO deal with the regulatory and legislative changes that occur frequently in its oversight areas.

The ERCO will provide expertise and coaching to assist management with functions such as identifying risks at the enterprise and division level, developing risk mitigation plans, following up on the outstanding audit findings, and performing evaluation of controls. Additionally, the ERCO will facilitate discussions and development of risk management, collect information, and prepare documents to support management.

B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

- ☑ Program is directly related to department's primary mission and is critical to achieving the department's goals.
- ☐ Program is indirectly related to department's primary mission.
- ☐ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description:

The ERCO's main function is to be responsible for assisting with the development of a governance risk management strategy to identify, evaluate, mitigate, and monitor the STO's operational and strategic risk and risk management tools, practices, and policies. Because STO has very dynamic and diverse program areas that directly play a vital role in California's economy, unmitigated risks can compromise the organization's ability to achieve its mission. The ERCO will support the STO and its BCAs with better understanding and evaluating the STO's risks and mitigation planning. The ERCO will focus on training, coaching, and assisting management with the creation of a risk framework that identifies, analyzes, evaluates, treats, monitors, and reviews, along with a risk mitigation strategy that will result in a better risk aggregation process across the organization.

It is critical that the STO establish this ERCO position to help management ensure risks are adequately documented and mitigated and controls are in place to protect the interests of the people of the State of California. The STO management needs expertise and assistance to adequately monitor and address risks. The ERCO will help management to engage in proactive and adequate monitoring of risks of the STO's day to day operations and regulatory oversight of the organization. This will allow management to focus on the highest risk and develop plans to immediately address compliance issues before they arise. In addition, the ERCO will be able to track and monitor compliance with prior and future audit recommendations to ensure they are addressed with appropriate remediation, thereby reducing risk to the STO and its BCAs.

B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

The STO does not currently have an established risk and compliance officer. The recent history of the STO includes four audits performed by the California State Auditor, eighteen audits by control agencies (i.e. Department of General Services, State Personnel Board, Department of the Military, etc.), annual audits of four BCAs in compliance with Government Code §5872 (SB 99/Chapter 557, 2009), annual audits of three BCAs per statute, annual audit in accordance with Government Code §13299.1 (securities accountability of the STO), and proposed legislation to restructure two of the BCAs. Because an established risk and compliance program addresses risks before they become problems, issues which were identified in some of these various audits, and/or legislative proposals might have been prevented had such a program been in place.

The STO has very dynamic and diverse program areas that play a vital role in California's economy. The STO is the state's banker, tasked with protecting the public's funds. The STO manages approximately $3.2 trillion in banking transactions, sells bonds and manages bond debt, and manages the state's investment portfolio, which has averaged more than $100 billion in assets over the past few years. Similarly, the BCAs serve the public, hospitals, businesses, and help spur housing and economic development. The risks involving these programs change constantly over time either in the technology (e.g., cyber security), oversight, or the legislation area, requiring continuous attention. A strong process which concentrates on enterprise-wide risks, not only addresses these risks, but also has the potential to identify and achieve cost efficiencies.

The STO has prioritized organization-wide compliance and transparency. As such, the creation of a CEA for this program will allow for an enterprise-wide risk assessment process that includes developing a risk management strategy, policies, procedures, and tools; monitoring and reporting risk, as well as oversight of the enterprise-wide risk assessment process. Unmitigated risks can compromise the organization's ability to achieve its mission. More importantly, the severity of risks can affect the state in many ways. If problems occur related to STO oversight or operations, it can lead to reputational damage, reflect poorly on the state, and could potentially have far-reaching consequences (e.g. cyber intrusion impacting State's financial services sector).

C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

The Enterprise Risk and Compliance Officer (ERCO) will be responsible for assisting with the development of a governance risk management strategy to identify, evaluate, mitigate, and monitor the STO's operational and strategic risk and risk management tools, practices, and policies. The compliance functions of the ERCO will include making recommendations on standards and procedures in identifying, preventing, detecting, and correcting noncompliance with applicable rules and regulations. Additionally, the ERCO will coordinate and serve as the STO's liaison for external audits. The ERCO will assist management in verifying internal controls in those areas with audit findings and assist with developing risk mitigation strategies. The specific policy functions that the ERCO will oversee are:

1. Risk Framework and Risk Management - The ERCO is responsible for development, coordination, and promulgation of the Risk Management Framework policy. For example, this policy will include developing training programs and implementing management systems that are capable of identifying, monitoring, and reporting documented, new or emerging risks. The ERCO will support the STO with better utilizing its resources, understanding organization-wide what needs to be done, and identifying the high-risk areas with the most opportunity for mitigation. The management's risk assessment process will provide a listing of risks on which to develop an on-going strategy in treating potential risk factors. The enterprise risk assessment will prevent past problems from reoccurring and takes a proactive approach to resolving problems before they occur. In addition, the risk assessment will provide the STO with a blueprint of its operations, risks, and controls. The risk process can measure risk to the organization by looking at factors such as: Velocity of the risk—how quickly it will occur; impact—short, medium, long-term effect; probability—how likely it is to occur; and risk appetite—how much risk can it take on without detriment to the entity.

2. Compliance - The ERCO will integrate a Risk Compliance Management Policy to ensure that the compliance programs throughout the organization are effective and efficient in identifying, preventing, detecting, and correcting noncompliance with applicable rules and regulations. Compliance risk is the risk of legal or regulatory sanctions, financial loss, or loss to reputation an entity may suffer as a result of its failure to comply with laws, regulations, rules, related self-regulatory organization standards, and codes of conduct applicable to its activities. It includes the potential for an adverse impact to clients and stakeholders of STO. The ERCO will facilitate discussions and development of risk management, coach management, collect information, determine why processes are working or not working, and make recommendations/suggest improvements. Additionally, the ERCO will implement principles and measures that are designed to minimize compliance risks and prevent violations of laws and regulations

3. Cybersecurity - The ERCO will develop and maintain an Information Security Risk Management Policy to frame, assess, respond, and monitor risk. For example: This policy applies to all electronic data created, stored, processed or transmitted by the STO and the Information Systems used with that data. Given the threat of increasingly sophisticated cyber-attacks aimed at breaching and damaging computer networks and infrastructure in California, the ERCO will work in coordination with the STO's Information Security Office to ensure that the organization meets the information security requirements published in the SAM, Section 5300 Information Security Policies.

In summary, ERCO will assist in the reduction of high-risk issues in the STO through the establishment of a risk group comprised of representatives from each division and BCA to discuss operational, compliance, safety, and strategic risks before they escalate. The ERCO will provide coaching and training to help the Executive Office, STO management, and staff of all levels to successfully identify, assess, and make decisions about risk. Lastly, STO wide policies and procedures providing efficiency and effectiveness in addressing risk mitigation will be institutionalized. The ERCO will be able to track and monitor compliance with prior and future audit recommendations to ensure they are addressed with appropriate remediation, thereby reducing risk to the STO and its BCAs.

C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

This ERCO will report to the Executive Office, specifically the Chief Deputy Treasurer, both functionally and administratively. This position will influence the enterprise and mission of STO. The scope of the ERCO's work will require training, coaching, facilitating, implementing policies, assisting, and documenting to provide informed input to management. In addition, engaging all staff within the STO, in risk discussions to uncover risks from all levels of the STO would be invaluable for Executive Management. The ERCO will provide expertise and coaching to assist management with several functions:

- Identify risks at the enterprise and division level.
- Development of risk mitigation plans.
- Follow up on the outstanding audit findings.
- Perform evaluation of controls.
- Implement procedures to ensure that the compliance programs throughout the organization are effective and efficient in identifying, preventing, detecting, and correcting noncompliance with applicable rules and regulations.
- Work on special projects at the direction of STO management.

Additionally, given the threat of increasingly sophisticated cyber-attacks aimed at breaching and damaging computer networks and infrastructure in California, the ERCO will work in coordination with the STO's Information Security Office to ensure that the organization meets the information security requirements published in the SAM, Section 5300 Information Security.

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

The CEA position will be developing and implementing new policy. As stated previously, this is a newly established program that has not been in place previously. The ERCO will be developing and implementing new policies that will directly impact the way that STO monitors, reports, and manages risk.